PAPER Special Issue on SITA

Secret Key Agreement from Correlated Gaussian Sources by Rate Limited Public Communication*

Shun WATANABE[†a)] ***and*** **Yasutada OOHAMA**[†b)], ***Members***

SUMMARY We investigate the secret key agreement from correlated Gaussian sources in which the legitimate parties can use the public communication with limited rate. For the class of protocols with the one-way public communication, we show a closed form expression of the optimal trade-off between the rate of key generation and the rate of the public communication. Our results clarify an essential difference between the key agreement from discrete sources and that from continuous sources.

key words: *Bin Coding, Gaussian Sources, Privacy Amplification, Quantization, Rate Limited Public Communication, Secret Key Agreement*

1. Introduction

Key agreement is one of the most important problems in the cryptography, and it has been extensively studied in the information theory for discrete sources (e.g. [1], [11], [12]) since the problem formulation by Maurer [19]. Recently, the confidential message transmission [10], [26] in the MIMO wireless communication has attracted considerable attention as a practical problem setting (e.g. [7], [17], [18]). Although the key agreement in the context of the wireless communication has also attracted considerable attention recently [6], the key agreement from analog sources has not been studied sufficiently compared to the confidential message transmission. As a fundamental case of the key agreement from analog sources, we consider the key agreement from correlated Gaussian sources in this paper. More specifically, we consider the problem in which the legitimate parties, Alice and Bob, and an eavesdropper, Eve, have correlated Gaussian sources respectively, and Alice and Bob share a secret key from their sources by using the public communication. Recently, the key agreement from Gaussian sources has attracted considerable attention in the context of the quantum key distribution [13], which is also a motivation to investigate the present problem.

Typically, the first step of the key agreement protocol from analog sources is the quantization of the sources. In the literatures (e.g. see [2], [3], [6]), the scalar quantizer is used, i.e., the observed source is quantized in each time instant. Using the finer quantization, we can expect the higher key rate in the protocol, where the key rate is the ratio between the length of the shared key and the block length of the sources that are used in the protocol. However, there is a problem such that the finer quantization might increase the rate of the public communication in the protocol. Although the public communication is usually regarded as a cheap resource in the context of the key agreement problem, it is limited by a certain amount in practice. Therefore, we consider the key agreement protocols with the rate limited public communication in this paper. The purpose of this paper is to clarify the optimal trade-off between the key rate and the public communication rate of the key agreement protocol from Gaussian sources. It should be emphasized that we consider the optimal trade-off among the protocols with not only the scalar quantizer but also the vector quantizer.

The key agreement by rate limited public communication was first studied by Csiszár and Narayan for discrete sources [11]. For the class of protocols with the one-way public communication, they characterized the optimal trade-off between the key rate and the public communication rate in terms of information theoretic quantities, i.e., they derived the so-called single letter characterization. However, there are two difficulties to extend their result to the Gaussian sources.

First, the direct part of the proof in [11] heavily relies on the finiteness of the alphabets of the sources, and cannot be applied to continuous sources. We show the direct part by using a method that is similar to the information spectrum approach [14].

Second, although the converse part of Csiszár and Narayan's characterization can be easily extended to continuous sources, the characterization is not computable because the characterization involves auxiliary random variables and the ranges of those random variables are unbounded for continuous sources. In this paper, we show that Gaussian auxiliary random variables are sufficient, and we derive a closed form expression of the optimal trade-off. A key tool in the derivation of the closed form expression is the entropy power inequality [9], which has been applied to solve the Gaussian multiterminal problems in the literatures [5], [16],

Manuscript received February 1, 2010.
Manuscript revised June 25, 2010.
[†]The authors are with the Department of Information Science and Intelligent Systems, University of Tokushima
*A part of this paper was presented at the 32nd symposium on information theory and its application.
a) E-mail: shun-wata@is.tokushima-u.ac.jp
b) E-mail: oohama@is.tokushima-u.ac.jp
DOI: 10.1587/transfun.E0.A.1

[22], [23].

There is another work that is related to this paper. Nitinawarat studied the problem in which Alice and Bob have correlated Gaussian sources and they share a secret key from their sources by the public communication [21]. The problem formulation in this paper can be regarded as a generalization of [21] to the case in which Eve also has a Gaussian source. It should be noted that [21] considered the key agreement with the rate limited quantization instead of the rate limited public communication.

The rest of this paper is organized as follows. In Section 2, we formulate the problem treated in this paper. Main results and the outlines of their proofs are presented in Section 3. Conclusions are discussed in Section 4, and the details of the proofs are presented in Appendices.

2. Preliminaries

Let X, Y, and Z be zero-mean correlated Gaussian sources on the set of real numbers $\mathbb{R}$ respectively. Then, let X^n, Y^n, and Z^n be i.i.d. copies of X, Y, and Z respectively. We assume that Alice, Bob, and Eve know the covariance matrix of (X,Y,Z). Throughout the paper, upper case letters indicate random variables, and the corresponding lower case letters indicate their realizations. We use the same notations as [9] for the entropy, the mutual information, etc..

Although Alice and Bob can use the public communication interactively in general, we concentrate on the class of key agreement protocols in which only Alice sends a message to Bob over the public channel†. First, Alice computes the message C_n from X^n and sends the message to Bob over the public channel. Then, she also compute the key S_n. Bob computes the key S_n' from Y^n and C_n.

The error probability of the protocol is defined by

$$\varepsilon_n := \Pr\{S_n \neq S_n'\}.$$

The security of the protocol is measured by the quantity

$$\nu_n := \log|\mathcal{S}_n| - H(S_n|C_n, Z^n), \tag{1}$$

where $\mathcal{S}_n$ is the range of the key S_n, and $|\mathcal{S}_n|$ indicates the cardinality of the set $\mathcal{S}_n$.

In this paper, we are interested in the trade-off between the public communication rate R_p and the key rate R_k. The rate pair (R_p, R_k) is defined to be achievable if there exists a sequence of protocols satisfying

$$\lim_{n\to\infty} \varepsilon_n = 0, \tag{2}$$

$$\lim_{n\to\infty} \nu_n = 0, \tag{3}$$

$$\limsup_{n\to\infty} \frac{1}{n}\log|\mathcal{C}_n| \le R_p, \tag{4}$$

$$\liminf_{n\to\infty} \frac{1}{n}\log|\mathcal{S}_n| \ge R_k, \tag{5}$$

where $\mathcal{C}_n$ is the range of the message C_n transmitted over the public channel. Then, the achievable rate region is defined as

$$\mathcal{R}(X,Y,Z) := \{(R_p,R_k) : (R_p,R_k) \text{ is achievable}\}.$$

The purpose of this paper is to derive a closed form expression of the rate region $\mathcal{R}(X,Y,Z)$.

3. Main Results

3.1 Statement of Results

In this section, we show a closed form expression of the rate region $\mathcal{R}(X,Y,Z)$, which will be proved in the next section. Let

$$\Sigma = \begin{bmatrix} \Sigma_x & \Sigma_{xy} & \Sigma_{xz} \\ \Sigma_{yx} & \Sigma_y & \Sigma_{yz} \\ \Sigma_{zx} & \Sigma_{zy} & \Sigma_z \end{bmatrix}$$

be the covariance matrix of (X,Y,Z). Throughout the paper, we assume that Σ is positive definite and $\Sigma_{xy} \neq 0$ because the key agreement is obviously impossible if $\Sigma_{xy} = 0$. Then, we can write (see Appendix C.1)

$$X = K_{xz}Z + W_1, \tag{6}$$

$$Y = K_{yx}X + K_{yz}Z + W_2 \tag{7}$$

$$= (K_{yx}K_{xz} + K_{yz})Z + K_{yx}W_1 + W_2, \tag{8}$$

where W_1 and W_2 are zero-mean Gaussian random variables independent of each other, W_1 is independent of Z, and W_2 is independent of (X,Z). The coefficients are given by

$$K_{xz} = \Sigma_{xz}\Sigma_z^{-1}$$

and

$$\begin{bmatrix} K_{yz} & K_{yx} \end{bmatrix} = \begin{bmatrix} \Sigma_{yz} & \Sigma_{yx} \end{bmatrix} \begin{bmatrix} \Sigma_z & \Sigma_{zx} \\ \Sigma_{xz} & \Sigma_x \end{bmatrix}^{-1}.$$

Furthermore, we also have

$$\Sigma_{W_1} = \Sigma_{x|z} = \Sigma_x - K_{xz}\Sigma_{zx}, \tag{9}$$

$$\Sigma_{W_2} = \Sigma_{y|xz} = \Sigma_y - K_{yx}\Sigma_{xy} - K_{yz}\Sigma_{zy}, \tag{10}$$

$$\Sigma_{y|z} = \Sigma_y - \Sigma_{yz}\Sigma_z^{-1}\Sigma_{zy}, \tag{11}$$

where Σ_{W_1} and Σ_{W_2} are the variances of W_1 and W_2 respectively, $\Sigma_{x|z}$ is the conditional variance of X given Z, $\Sigma_{y|xz}$ and $\Sigma_{y|z}$ are the conditional variances of Y given (X,Z) and Z respectively.

For $R_p \ge 0$, let

$$R_k(R_p) := \sup\{R_k : (R_k, R_p) \in \mathcal{R}(X,Y,Z)\}.$$

Before investigating the rate region, we present well

†It should be noted that the results in this paper is valid for the class of key agreement protocols in which only Bob sends a message to Alice.

known upper bound on the function $R_k(R_p)$, which was shown for the discrete sources in [1], [19], and can be shown in a similar manner for continuous sources.

Proposition 1 ([1], [19]) For any $R_p \geq 0$, we have

$$R_k(R_p) \leq I(X;Y|Z) = \frac{1}{2}\log\frac{\Sigma_{y|z}}{\Sigma_{y|xz}}. \tag{12}$$

Remark 2 Although we will concentrate on the class of key agreement protocols in which only Alice sends a message to Bob over the public channel, the upper bound in Proposition 1 is still valid even if we consider the class of protocols in which Alice and Bob sends messages interactively.

Remark 3 In Eq. (12), we use the fact that (X,Y,Z) are Gaussian only to derive the right equality, and the left inequality holds for any continuous sources.

We first consider the case such that the sources are degraded, i.e., they satisfy the Markov chain

$$X \leftrightarrow Y \leftrightarrow Z.$$

Theorem 4 Suppose that (X,Y,Z) are degraded. Then, we have

$$\mathcal{R}(X,Y,Z) = \Bigg\{(R_p,R_k): R_k \leq \frac{1}{2}\log\frac{\Sigma_{y|xz}e^{-2R_p}+\Sigma_{y|z}\left(1-e^{-2R_p}\right)}{\Sigma_{y|xz}}\Bigg\}. \tag{13}$$

As we can find from the above theorem, the function $R_k(R_p)$ is concave and monotonically increasing, and it converges to the upper bound in Proposition 1 as R_p goes to infinity.

Remark 5 When (X,Y,Z) are discrete sources and are degraded, it is known [1], [11] that

$$R_k(R_p) = I(X;Y|Z).$$

for any $R_p \geq H(X|Y)$. Furthermore for $R_p \geq H(X|Y)$, $R_k(R_p)$ can be achieved by the combination of the Slepian-Wolf coding [24] and the privacy amplification (e.g. see [4]), and the quantization of Alice's source is not necessary. On the other hand, Theorem 4 implies

$$R_k(R_p) < I(X;Y|Z)$$

for any finite R_p. This fact suggests an essential difference between the key agreement from discrete sources and that from continuous sources.

When we consider the protocol with only one-way public communication, note that the error probability ε_n and the security parameter ν_n only depend on the marginal densities $p(x,y)$ and $p(x,z)$ respectively. More precisely, let $(\bar{X},\bar{Y},\bar{Z})$ be random variables such that the marginal densities of (X,Y) and $(\bar{X},\bar{Y})$, and those of (X,Z) and $(\bar{X},\bar{Z})$ coincide respectively. Then we have

$$\mathcal{R}(X,Y,Z) = \mathcal{R}(\bar{X},\bar{Y},\bar{Z}).$$

By using this fact and the following lemma, the proof of which will be presented in Appendix C.2, we can always reduce the general case to the degraded case.

Lemma 6 If the square of the correlation coefficient of (X,Y) is larger than that of (X,Z), i.e.,

$$\Sigma_{xy}^2\Sigma_y^{-1}\Sigma_x^{-1} > \Sigma_{xz}^2\Sigma_z^{-1}\Sigma_x^{-1}, \tag{14}$$

then there exist jointly Gaussian sources $(\bar{X},\bar{Y},\bar{Z})$ such that

$$\bar{X} \leftrightarrow \bar{Y} \leftrightarrow \bar{Z} \tag{15}$$

is satisfied, and that the marginal densities of (X,Y) and $(\bar{X},\bar{Y})$, and those of (X,Z) and $(\bar{X},\bar{Z})$ coincide respectively.

On the other hand, if the square of the correlation coefficient of (X,Y) is smaller than or equal to that of (X,Z), i.e.,

$$\Sigma_{xy}^2\Sigma_y^{-1}\Sigma_x^{-1} \leq \Sigma_{xz}^2\Sigma_z^{-1}\Sigma_x^{-1}, \tag{16}$$

then there exist (not necessarily Gaussian) sources $(\bar{X},\bar{Y},\bar{Z})$ such that

$$\bar{X} \leftrightarrow \bar{Z} \leftrightarrow \bar{Y} \tag{17}$$

is satisfied, and that the marginal densities of (X,Y) and $(\bar{X},\bar{Y})$, and those of (X,Z) and $(\bar{X},\bar{Z})$ coincide respectively.

When there are jointly Gaussian sources $(\bar{X},\bar{Y},\bar{Z})$ satisfying Eq. (15), we can compute the region by using Theorem 4. On the other hand, when there are $(\bar{X},\bar{Y},\bar{Z})$ satisfying Eq. (17), Proposition 1 implies $R_k(R_p) = 0$ for any $R_p \geq 0$.

3.2 Proof of Theorem 4

3.2.1 Converse Part

In order to prove the converse part, we need the following proposition and corollary. The proposition was shown for discrete sources in [11, Theorem 2.6], and it can be shown almost in the same manner for continuous sources.

Proposition 7 ([11]) Suppose that a rate pair (R_p,R_k) is included in $\mathcal{R}(X,Y,Z)$. Then, there exist auxiliary random variables U and V satisfying

$$R_p \geq I(U;X|Y), \tag{18}$$

$$R_k \leq I(U;Y|V) - I(U;Z|V), \tag{19}$$

and the Markov chain

$$V \leftrightarrow U \leftrightarrow X \leftrightarrow (Y, Z). \tag{20}$$

For degraded sources, we can simplify the above proposition, which will be shown in Appendix B.

Corollary 8 Suppose that (X, Y, Z) is degraded, i.e., $X \leftrightarrow Y \leftrightarrow Z$. If $(R_p, R_k) \in \mathcal{R}(X, Y, Z)$, then there exists an auxiliary random variable U satisfying

$$R_p \geq I(U; X|Y), \tag{21}$$
$$R_k \leq I(U; Y|Z), \tag{22}$$

and the Markov chain

$$U \leftrightarrow X \leftrightarrow Y \leftrightarrow Z. \tag{23}$$

Proof of Converse Part)

Part of ideas of the following proof are borrowed from [25] with proper modifications. In the following, $h(\cdot)$ and $h(\cdot|\cdot)$ designate the differential entropy and the conditional differential entropy respectively [9].

We will show

$$R_p \geq \frac{1}{2} \log \frac{\Sigma_{y|z} - \Sigma_{y|xz}}{\Sigma_{y|z} e^{-2R_k} - \Sigma_{y|xz}} - R_k. \tag{24}$$

Then, by solving the inequality with respect to R_k, we have the converse part of Theorem 4.

For any auxiliary random variable U satisfying Eq. (23), by a straightforward calculation, we have

$$\begin{aligned} &h(Y|Z) - I(U; Y|Z) \\ &= h(Y|U, Z) \\ &= h(K_{yx}X + K_{yz}Z + W_2|U, Z) \\ &= h(K_{yx}X + W_2|U, Z). \end{aligned}$$

Then, by using the conditional version of the entropy power inequality (EPI) [5], we have

$$\begin{aligned} &\exp\left[2h(K_{yx}X + W_2|U, Z)\right] \\ &\geq \exp\left[2h(K_{yx}X|U, Z)\right] + \exp\left[2h(W_2)\right] \\ &= K_{yx}^2 \exp\left[2h(X|U, Z)\right] + \exp\left[2h(W_2)\right] \\ &= K_{yx}^2 \exp\left[-2I(U; X|Z) + 2h(X|Z)\right] \\ &\quad + \exp\left[2h(W_2)\right] \\ &= K_{yx}^2 \exp\left[-2I(U; X|Z) + 2h(W_1)\right] \\ &\quad + \exp\left[2h(W_2)\right]. \end{aligned}$$

Thus, we have

$$\begin{aligned} &I(U; X|Z) - I(U; Y|Z) \\ &\geq \frac{1}{2} \log \left[K_{yx}^2 \exp\{2h(W_1)\}\right] \\ &\quad -\frac{1}{2} \log \left[\exp\{2h(Y|Z) - 2I(U; Y|Z)\}\right. \\ &\quad \left. - \exp\{2h(W_2)\}\right] - I(U; Y|Z). \end{aligned} \tag{25}$$

From Eqs. (10) and (8), we can find that the variances of W_2 and $K_{yx}W_1$ are $\Sigma_{y|xz}$ and $K_{yx}^2 \Sigma_{W_1} = \Sigma_{y|z} - \Sigma_{y|xz}$ respectively. Thus, we can rewrite the right hand side of Eq. (25) as

$$\frac{1}{2} \log \frac{\Sigma_{y|z} - \Sigma_{y|xz}}{\Sigma_{y|z} e^{-2I(U;Y|Z)} - \Sigma_{y|xz}} - I(U; Y|Z).$$

Since the function

$$\frac{1}{2} \log \frac{\Sigma_{y|z} - \Sigma_{y|xz}}{\Sigma_{y|z} e^{-2a} - \Sigma_{y|xz}} - a$$

is monotonically increasing for $0 \leq a \leq I(X; Y|Z)$ and

$$I(U; X|Z) - I(U; Y|Z) = I(U; X|Y)$$

for (U, X, Y, Z) satisfying Eq. (23), Corollary 8 implies Eq. (24). □

3.2.2 Direct Part

In order to prove the direct part, we need the following proposition, which can be regarded as a generalization of [11, Theorem 2.6] to continuous sources†. We show a proof in Appendix A because the proof of [11, Theorem 2.6] heavily relies on the finiteness of the alphabets and its generalization to continuous sources seems nontrivial. It should be noted that the following proposition holds for non-degraded case.

Proposition 9 For an auxiliary random variable U satisfying the Markov chain

$$U \leftrightarrow X \leftrightarrow (Y, Z), \tag{26}$$

let (R_p, R_k) be a rate pair such that

$$\begin{aligned} R_p &\geq I(U; X) - I(U; Y), \\ R_k &\leq I(U; Y) - I(U; Z). \end{aligned}$$

Then, we have $(R_p, R_k) \in \mathcal{R}(X, Y, Z)$.

Note that

$$\begin{aligned} I(U; X|Y) &= I(U; X) - I(U; Y), \\ I(U; Y|Z) &= I(U; Y) - I(U; Z) \end{aligned}$$

for degraded sources.

Proof of Direct Part)

Let W be a zero mean Gaussian random variable, and $U = X + W$. Since the (conditional version of) entropy power inequality holds with equality for Gaussian random variables [5], [9], Eq. (25) in the converse part holds with equality, i.e., we have

†Although [11, Theorem 2.6] involves two auxiliary random variables, we only show the version with only one auxiliary random variable because one of the auxiliary random variables in [11, Theorem 2.6] is not needed to show Theorem 4.

$$\begin{aligned} & I(U;X|Y) \\ & = I(U;X|Z) - I(U;Y|Z) \\ & = \frac{1}{2}\log\frac{\Sigma_{y|z}-\Sigma_{y|xz}}{\Sigma_{y|z}e^{-2I(U;Y|Z)}-\Sigma_{y|xz}} - I(U;Y|Z). \end{aligned}$$

Thus, by setting $I(U;Y|Z) = R_k$ and $I(U;X|Y) = R_p$, by solving the equality with respect to R_k, and by adjusting the variance of W, we find that any (R_p, R_k) satisfying the equality

$$R_k = \frac{1}{2}\log\frac{\Sigma_{y|xz}e^{-2R_p}+\Sigma_{y|z}(1-e^{-2R_p})}{\Sigma_{y|xz}}$$

is achievable. □

4. Conclusions and Discussions

We investigated the secret key agreement from Gaussian sources by rate limited public communication. For the class of protocols with the one-way public communication, we derived a closed form expression of the optimal trade-off between the key rate and the public communication rate. The optimal trade-off for the class of protocols with the two-way public communication remains unsolved and investigating it is a future research agenda.

Our result suggested an essential difference between the key agreement from discrete sources and that from continuous sources (Remark 5). For discrete sources, if the public communication rate is larger than $H(X|Y)$, the upper bound can be achieved without quantization. On the other hand for Gaussian sources, the upper bound cannot be achieved for any finite public communication rate.

The problem formulation treated in this paper can be regarded as Gaussian version of the source type model [1]. We can also consider Gaussian version of the channel type model. In such a model, Alice can send a signal, with power constraint, to Bob and Eve over Gaussian channels. In addition to the Gaussian channel, Alice and Bob can use the public communication with limited rate. For the class of protocols with the forward public communication[†], by a slight modification of the proof of [1, Theorem 2], we can show that the supremum of achievable key rates coincides with the secrecy capacity of the Gaussian wiretap channel [16] no matter what the limitation of the public communication rate.

Appendix A: Proof of Proposition 9

For arbitrarily fixed auxiliary random variable satisfying Eq. (26), we show that the rate pair

[†]The forward (backward) public communication means that only Alice (Bob) sends a public message to Bob (Alice). It should be noted that the forward public communication and the backward public communication make significant difference for the channel type model.

$$\begin{aligned} R_p &= I(U;X) - I(U;Y) + 4\gamma, \\ R_k &= I(U;Y) - I(U;Z) - 6\gamma \end{aligned}$$

is achievable for any $\gamma > 0$. Instead of showing the achievability for the security criterion defined by Eq. (1), we show the achievability for the security criterion defined by

$$\mu_n := \int p(z^n) \| P_{S_n C_n|Z^n}(\cdot,\cdot|z^n) - P_{\bar{S}_n}(\cdot)P_{C_n|Z^n}(\cdot|z^n)\| dz^n,$$

where $P_{\bar{S}_n}$ is the uniform distribution on the key alphabet $\mathcal{S}_n$, and $\|\cdot\|$ is the variational distance [9]. More precisely, we show that there exists a sequence of protocols satisfying Eqs. (2), (4) and (5) and μ_n converges to 0 exponentially. Then, by using [20, Lemma 3], we can also show that ν_n also converges to 0.

Our protocol roughly consists of three steps: the quantization, the bin coding [9], and the privacy amplification. First, Alice quantizes her source by a function $g_n : \mathbb{R}^n \to \mathcal{Q}_n \subset \mathbb{R}^n$. We use the auxiliary random variable U for quantization almost in a similar manner as the Wyner-Ziv problem [27]. After the quantization, she sends the bin index $C_n = \phi_n(g_n(X^n))$ by a function $\phi_n : \mathcal{Q}_n \to \mathcal{C}_n$. Bob decodes the index and his source by a function $\psi_n : \mathcal{C}_n \times \mathbb{R}^n \to \mathcal{Q}_n$. Note that the public communication rate R_p must be large enough so that Bob can recover the quantized source by using his source Y^n as side-information at the decoder. Finally, they obtain keys $S_n = f_n(g_n(X^n))$ and $S_n' = f_n(\psi_n(\phi_n(C_n), Y^n))$ by a function $f_n : \mathcal{Q}_n \to \mathcal{S}_n$ respectively. Existence of functions $\{(g_n, \phi_n, \psi_n, f_n)\}_{n=1}^{\infty}$ satisfying Eqs. (2), (4) and (5) and $\mu_n \to 0$ are guaranteed by the following lemmas. Lemma 10 is the so-called Markov lemma, the proof of which will be omitted (e.g. see [15]). In order to upper bound the error probability ε_n, we need Lemma 11, which appears in the course of deriving the general formula of the Wyner-Ziv problem [15]. We also omit the proof. In order to upper bound the security parameter μ_n, we need Lemma 12, which is an extension of the privacy amplification lemma shown in [20, Lemma 4]. Since we apply the privacy amplification to the (vector) quantized source in our protocol, we need Lemma 12. The proof of Lemma 12 is the most difficult part of the proof of Proposition 9, and it will be proved in the next section.

For a fixed auxiliary random variable U satisfying Eq. (26) and $t, \alpha, \beta \in \mathbb{R}$, let

$$\begin{aligned} \mathcal{T}_n &:= \left\{ (u^n, x^n) : \frac{1}{n}\log\frac{p(u^n|x^n)}{p(u^n)} \le t \right\}, \\ \mathcal{A}_n &:= \left\{ (u^n, y^n) : \frac{1}{n}\log\frac{p(y^n|u^n)}{p(y^n)} \ge \alpha \right\}, \\ \mathcal{B}_n &:= \left\{ (u^n, x^n, z^n) : \frac{1}{n}\log\frac{p(x^n|u^n,z^n)}{p(x^n|z^n)} \ge \beta \right\}. \end{aligned}$$

Lemma 10 For any $t, \alpha, \beta \in \mathbb{R}$, there exists a function $g_n : \mathbb{R}^n \to \mathcal{Q}_n$ such that

$$\begin{aligned}&\Pr\{(g_n(X^n), Y^n) \notin \mathcal{A}_n \text{ or } (g_n(X^n), X^n, Z^n) \notin \mathcal{B}_n\}\\ &\le 2\sqrt{\delta_n} + \Pr\{(U^n, X^n) \notin \mathcal{T}_n\} + \exp\{-|\mathcal{Q}_n|e^{-tn}\},\end{aligned}$$

where

$$\delta_n := \Pr\{(U^n, Y^n) \notin \mathcal{A}_n \text{ or } (U^n, X^n, Z^n) \notin \mathcal{B}_n\}.$$

Lemma 11 For any function $g_n : \mathbb{R}^n \to \mathcal{Q}_n$ and $\alpha \in \mathbb{R}$, there exist functions $\phi_n : \mathcal{Q}_n \to \mathcal{C}_n$ and $\psi_n : \mathcal{C}_n \times \mathbb{R}^n \to \mathcal{Q}_n$ such that

$$\begin{aligned}&\Pr\{g_n(X^n) \neq \psi_n(\phi_n(g_n(X^n)), Y^n)\}\\ &\le \frac{|\mathcal{Q}_n|}{|\mathcal{C}_n|}e^{-\alpha n} + \Pr\{(g_n(X^n), Y^n) \notin \mathcal{A}_n\}.\end{aligned}$$

Lemma 12 For any functions $g_n : \mathbb{R}^n \to \mathcal{Q}_n$, $\phi_n : \mathcal{Q}_n \to \mathcal{C}_n$, and $\beta \in \mathbb{R}$, there exists a function $f_n : \mathcal{Q}_n \to \mathcal{S}_n$ such that

$$\mu_n \le \sqrt{|\mathcal{S}_n||\mathcal{C}_n|e^{-\beta n}} + 2\Pr\{(g_n(X^n), X^n, Z^n) \notin \mathcal{B}_n\}.$$

Note that only the cardinality of $\mathcal{C}_n$ appears in the upper bound on μ_n no matter the structure of a specific function ϕ_n. However the functions f_n realizing the upper bound depend on the structure of ϕ_n.

From Lemmas 10, 11, and 12, by setting

$$\begin{aligned}|\mathcal{Q}_n| &= \exp\{n(I(U;X) + 2\gamma)\},\\ |\mathcal{C}_n| &= \exp\{n(I(U;X) - I(U;Y) + 4\gamma)\},\\ |\mathcal{S}_n| &= \exp\{n(I(U;Y) - I(U;Z) - 6\gamma)\},\\ t &= I(U;X) + \gamma,\\ \alpha &= I(U;Y) - \gamma,\\ \beta &= I(U;X|Z) - \gamma,\end{aligned}$$

and by noting that $I(U;X|Z) = I(U;X) - I(U;Z)$, we obtain a sequence of protocols satisfying Eqs. (2), (4) and (5) and μ_n exponentially[†] converges to 0. By using [20, Lemma 3], we can show that Eq. (3) is also satisfied.

Finally, by taking a sequence $\{\gamma_i\}$ such that $\gamma_1 > \gamma_2 > \cdots > 0$ and $\gamma_i \to 0$ $(i \to \infty)$ instead of $\gamma > 0$, and by using the diagonalization argument [14], we have Proposition 9. □

A.1 Proof of Lemma 12

In the following, we use the notation

$$f_n^{-1}(s) := \{u^n \in \mathcal{Q}_n : f_n(u^n) = s\}.$$

The sets $\phi_n^{-1}(c)$ for $c \in \mathcal{C}_n$ and $g_n^{-1}(u^n)$ for $u^n \in \mathcal{Q}_n$ are defined in similar manners. Furthermore, for a set $A \subset \mathcal{Q}_n$, we denote $g_n^{-1}(A) := \cup_{u^n \in A} g_n^{-1}(u^n)$. For a set $B \subset \mathbb{R}^n$, we define

$$P_{X^n|Z^n}(B|z^n) := \Pr\{X^n \in B | Z^n = z^n\}.$$

In this section, it should be also noted that summations are taken over the range of the indices unless otherwise specified.

For fixed $z^n \in \mathbb{R}^n$, let

$$\mathcal{B}_{z^n} := \{x^n : (g_n(x^n), x^n, z^n) \in \mathcal{B}_n\},$$

and $\mathcal{B}_{z^n}^c$ be the complement of $\mathcal{B}_{z^n}$ in $\mathbb{R}^n$. Then, by a straightforward calculation, we have

$$\begin{aligned}&\|P_{S_nC_n|Z^n}(\cdot,\cdot|z^n) - P_{\bar{S}_n}(\cdot)P_{C_n|Z^n}(\cdot|z^n)\|\\
&= \sum_{s,c} |P_{S_nC_n|Z^n}(s,c|z^n) - P_{\bar{S}_n}(s)P_{C_n|Z^n}(c|z^n)|\\
&= \sum_{s,c} |P_{X^n|Z^n}(g_n^{-1}(f_n^{-1}(s) \cap \phi_n^{-1}(c))|z^n)\\
&\quad - P_{\bar{S}_n}(s)P_{X^n|Z^n}(g_n^{-1}(\phi_n^{-1}(c))|z^n)|\\
&= \sum_{s,c} |P_{X^n|Z^n}(g_n^{-1}(f_n^{-1}(s) \cap \phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n)\\
&\quad - P_{\bar{S}_n}(s)P_{X^n|Z^n}(g_n^{-1}(\phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n)\\
&\quad + P_{X^n|Z^n}(g_n^{-1}(f_n^{-1}(s) \cap \phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}^c|z^n)\\
&\quad - P_{\bar{S}_n}(s)P_{X^n|Z^n}(g_n^{-1}(\phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}^c|z^n)|\\
&\le \sum_{s,c} |P_{X^n|Z^n}(g_n^{-1}(f_n^{-1}(s) \cap \phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n)\\
&\quad - P_{\bar{S}_n}(s)P_{X^n|Z^n}(g_n^{-1}(\phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n)|\\
&\quad + \sum_{s,c} |P_{X^n|Z^n}(g_n^{-1}(f_n^{-1}(s) \cap \phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}^c|z^n)\\
&\quad - P_{\bar{S}_n}(s)P_{X^n|Z^n}(g_n^{-1}(\phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}^c|z^n)|\\
&= \sum_{s,c} |P_{X^n|Z^n}(g_n^{-1}(f_n^{-1}(s) \cap \phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n)\\
&\quad - P_{\bar{S}_n}(s)P_{X^n|Z^n}(g_n^{-1}(\phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n)|\\
&\quad + 2P_{X^n|Z^n}(\mathcal{B}_{z^n}^c|z^n), \qquad (\text{A}\cdot 1)\end{aligned}$$

where we used the triangle inequality. By using the Cauchy-Schwarz inequality, the first term of Eq. (A·1) is upper bounded by

$$\begin{aligned}&\Bigg[|\mathcal{S}_n||\mathcal{C}_n| \sum_{s,c} |P_{X^n|Z^n}(g_n^{-1}(f_n^{-1}(s) \cap \phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n)\\
&\quad - P_{\bar{S}_n}(s)P_{X^n|Z^n}(g_n^{-1}(\phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n)|^2\Bigg]^{1/2}. \qquad (\text{A}\cdot 2)\end{aligned}$$

Furthermore, we can rewrite the inside of the square root of Eq. (A·2) as

$$\begin{aligned}&\sum_{s,c} |P_{X^n|Z^n}(g_n^{-1}(f_n^{-1}(s) \cap \phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n)\\
&\quad - P_{\bar{S}_n}(s)P_{X^n|Z^n}(g_n^{-1}(\phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n)|^2\end{aligned}$$

[†]We use the Chernoff bound (e.g. see [9]) instead of the Chebyshev inequality to upper bound δ_n and $\Pr\{(U^n, X^n) \notin \mathcal{T}_n\}$.

$$= \sum_{s,c} P_{X^n|Z^n}(g_n^{-1}(f_n^{-1}(s) \cap \phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n)^2 - \sum_c \frac{1}{|\mathcal{S}_n|} P_{\bar{S}_n}(s) P_{X^n|Z^n}(g_n^{-1}(\phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n)^2, \quad (A\cdot 3)$$

where we used the facts $P_{\bar{S}_n}(s) = \frac{1}{|\mathcal{S}_n|}$ and

$$\sum_s P_{X^n|Z^n}(g_n^{-1}(f_n^{-1}(s) \cap \phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n) = P_{X^n|Z^n}(g_n^{-1}(\phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n).$$

We can rewrite the first term of Eq. (A· 3) as

$$\sum_{s,c} P_{X^n|Z^n}(g_n^{-1}(f_n^{-1}(s) \cap \phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n)^2$$
$$= \sum_{s,c} \sum_{u^n, \hat{u}^n \in f_n^{-1}(s) \cap \phi_n^{-1}(c)} P_{X^n|Z^n}(g_n^{-1}(u^n) \cap \mathcal{B}_{z^n}|z^n) P_{X^n|Z^n}(g_n^{-1}(\hat{u}^n) \cap \mathcal{B}_{z^n}|z^n)$$
$$= \sum_{s,c} \sum_{u^n, \hat{u}^n \in \phi_n^{-1}(c)} \delta_{f_n(u^n), f_n(\hat{u}^n)} P_{X^n|Z^n}(g_n^{-1}(u^n) \cap \mathcal{B}_{z^n}|z^n) P_{X^n|Z^n}(g_n^{-1}(\hat{u}^n) \cap \mathcal{B}_{z^n}|z^n), \quad (A\cdot 4)$$

where $\delta_{a,b} = 1$ if $a = b$ and $\delta_{a,b} = 0$ otherwise. In a similar manner, we can rewrite the second term of Eq. (A· 3) as

$$\sum_c \frac{1}{|\mathcal{S}_n|} P_{\bar{S}_n}(s) P_{X^n|Z^n}(g_n^{-1}(\phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}^c|z^n)^2$$
$$= \sum_c \frac{1}{|\mathcal{S}_n|} \sum_{u^n, \hat{u}^n \in \phi_n^{-1}(v)} P_{X^n|Z^n}(g_n^{-1}(u^n) \cap \mathcal{B}_{z^n}|z^n) P_{X^n|Z^n}(g_n^{-1}(\hat{u}^n) \cap \mathcal{B}_{z^n}|z^n). \quad (A\cdot 5)$$

Let $\mathcal{F}_n$ be a universal hash family of functions from $\mathcal{Q}_n$ to $\mathcal{S}_n$ [8], i.e.,

$$P_{F_n}(\{f_n \in \mathcal{F}_n : f_n(u^n) = f_n(\hat{u}^n)\}) \le \frac{1}{|\mathcal{S}_n|}$$

for any distinct u^n and $\hat{u}^n$, where P_{F_n} is the uniform distribution on $\mathcal{F}_n$. Combining Eqs. (A· 3)–(A· 5), we can evaluate the inside of the square root of Eq. (A· 2) averaged over the random choice of f_n as follows:

$$\mathbb{E}_{f_n}\left[\sum_{s,c} P_{X^n|Z^n}(g_n^{-1}(f_n^{-1}(s) \cap \phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n)^2 - \sum_c \frac{1}{|\mathcal{S}_n|} P_{X^n|Z^n}(g_n^{-1}(\phi_n^{-1}(c)) \cap \mathcal{B}_{z^n}|z^n)^2\right]$$
$$= \sum_c \sum_{u^n, \hat{u}^n \in \phi_n^{-1}(c)} \mathbb{E}\left[\delta_{f_n(u^n), f_n(\hat{u}^n)} - \frac{1}{|\mathcal{S}_n|}\right] P_{X^n|Z^n}(g_n^{-1}(u^n) \cap \mathcal{B}_{z^n}|z^n) P_{X^n|Z^n}(g_n^{-1}(\hat{u}^n) \cap \mathcal{B}_{z^n}|z^n)$$
$$\le \sum_c \sum_{u^n \in \phi_n^{-1}(c)} P_{X^n|Z^n}(g_n^{-1}(u^n) \cap \mathcal{B}_{z^n}|z^n) P_{X^n|Z^n}(g_n^{-1}(u^n) \cap \mathcal{B}_{z^n}|z^n)$$
$$= \sum_{u^n \in \mathcal{Q}_n} P_{X^n|Z^n}(g_n^{-1}(u^n) \cap \mathcal{B}_{z^n}|z^n) P_{X^n|Z^n}(g_n^{-1}(u^n) \cap \mathcal{B}_{z^n}|z^n) \quad (A\cdot 6)$$

Since

$$p(x^n|z^n) \le p(x^n|u^n, z^n) e^{-\beta n}$$

for $(u^n, x^n, z^n) \in \mathcal{B}_n$, Eq. (A· 6) is upper bounded by

$$\sum_{u^n \in \mathcal{Q}_n} P_{X^n|Z^n}(g_n^{-1}(u^n) \cap \mathcal{B}_{z^n}|z^n) P_{X^n|U^n Z^n}(g_n^{-1}(u^n) \cap \mathcal{B}_{z^n}|u^n, z^n) e^{-\beta n}$$
$$\le \sum_{u^n \in \mathcal{Q}_n} P_{X^n|Z^n}(g_n^{-1}(u^n) \cap \mathcal{B}_{z^n}|z^n) e^{-\beta n}$$
$$\le e^{-\beta n}. \quad (A\cdot 7)$$

Since the square root function $\sqrt{\cdot}$ is concave, by combining Eqs. (A· 3)–(A· 7), Eq. (A· 2) averaged over f_n is upper bounded by $\sqrt{|\mathcal{S}_n||\mathcal{C}_n|e^{-\beta n}}$. By substituting this upper bound into Eq. (A· 1), by taking the average over $z^n \in \mathbb{R}^n$, and by using the concavity of $\sqrt{\cdot}$, we have

$$\mathbb{E}_{f_n}[\mu_n] \le \sqrt{|\mathcal{S}_n||\mathcal{C}_n|e^{-\beta n}} + 2\Pr\{(g_n(X^n), X^n, Z^n) \notin \mathcal{B}_n\}.$$

Thus, there exists at least one $f_n \in \mathcal{F}_n$ satisfying the statement of the lemma. □

Appendix B: Proof of Corollary 8

For any (U, V) satisfying Eqs. (18) and (20), we have

$$\begin{aligned} I(V;Y) + I(U;Y|V) &= I(U,V;Y) \\ &= I(U;Y) + I(V;Y|U) \\ &= I(U;Y), \end{aligned}$$

where the last equality follows from the fact that V, U, and Y form a Markov chain. Similarly, we have

$$I(V;Z) + I(U;Z|V) = I(U;Z).$$

Since we have

$$I(V;Y) \ge I(V;Z)$$

for degraded sources, we have

$$I(U;Y|V) - I(U;Z|V) \le I(U;Y) - I(U;Z),$$

which implies the assertion of the corollary. □

Appendix C: Miscellaneous Facts

For reader's convenience, we review some basic facts on

jointly Gaussian random variables.

C.1 Derivations of Eqs.(6)–(8)

The probability density function of zero-mean Gaussian random vector $\mathbf{X}$ is uniquely determined by its covariance matrix $\Sigma_{\mathbf{X}}$. Furthermore, for any non-degenerate matrix A, the covariance matrix of the Gaussian random vector $\mathbf{X}' = A\mathbf{X}$ is given by $\Sigma_{\mathbf{X}'} = A\Sigma_{\mathbf{X}}A^T$. On the other hand, any non-degenerate symmetric matrix of the form

$$M = \begin{bmatrix} A & B \\ B^T & C \end{bmatrix}$$

can be decomposed as

$$M = \begin{bmatrix} I & 0 \\ B^T A^{-1} & I \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & C - B^T A^{-1} B \end{bmatrix} \begin{bmatrix} I & A^{-1}B \\ 0 & I \end{bmatrix}.$$

By using these facts, we can derive Eqs.(6)–(8).

C.2 Proof of Lemma 6

By using facts in Appendix C.1, we can write

$$Y = \Sigma_{xy}\Sigma_x^{-1}X + N_y,$$
$$Z = \Sigma_{xz}\Sigma_x^{-1}X + N_z,$$

where N_y and N_z are Gaussian random variables that are independent of X and the variances are $\Sigma_y - \Sigma_{xy}^2\Sigma_x^{-1}$ and $\Sigma_z - \Sigma_{xz}^2\Sigma_x^{-1}$ respectively. When Eq. (14) is satisfied, by setting $\bar{X} = X$, $\bar{Y} = Y$, and

$$\bar{Z} = \Sigma_{xz}\Sigma_{xy}^{-1}\bar{Y} + \hat{N}$$

for Gaussian random variable $\hat{N}$ with variance $\Sigma_z - \Sigma_{xz}^2\Sigma_y\Sigma_{xy}^{-2}$, we obtain jointly Gaussian sources satisfying the assertion of the lemma, where $\hat{N}$ is independent of the other random variables. When Eq. (16) is satisfied with strict inequality, we can obtain jointly Gaussian sources satisfying the assertion of the lemma in a similar manner. When Eq. (16) is satisfied with equality, by setting $\bar{X} = X$, $\bar{Z} = Z$, and $\bar{Y} = \Sigma_{xy}\Sigma_{xz}^{-1}\bar{Z}$, we obtain sources (not jointly Gaussian because the covariance matrix is degenerated) satisfying the assertion of the lemma. □

Acknowledgment

The first author would like to thank Prof. Ryutaroh Matsumoto for valuable discussions and comments. We also thank the anonymous reviewers for their constructive comments and suggestions. This research is partly supported by Grant-in-Aid for Young Scientists (Start-up): KAKENHI 21860064.

References

[1] R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography–part I: Secret sharing,” IEEE Trans. Inform. Theory, vol.39, no.4, pp.1121–1132, July 1993.
[2] G.V. Assche, Quantum Cryptography and Secret-Key Distillation, Cambridge Univ. Press, 2006.
[3] G.V. Assche, J. Cardinal, and N.J. Cerf, “Reconciliation of a quantum-distributed Gaussian key,” IEEE Trans. Inform. Theory, vol.50, no.2, pp.394–400, February 2004.
[4] C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, “Generalized privacy amplification,” IEEE Trans. Inform. Theory, vol.41, no.6, pp.1915–1923, Nov. 1995.
[5] P.P. Bergmans, “A simple converse for broadcast channels with additive white Gaussian noise,” IEEE Trans. Inform. Theory, vol.20, no.2, pp.279–280, March 1974.
[6] M. Bloch, J. Barros, M.R.D. Rodrigues, and S.W. McLaughlin, “Wireless information-theoretic security,” IEEE Trans. Inform. Theory, vol.54, no.6, pp.2515–2534, June 2008.
[7] R. Bustin, R. Liu, H.V. Poor, and S. Shamai, “An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel,” EURASIP Journal on Wireless Communication and Networking, 2009.
[8] J.L. Carter and M.N. Wegman, “Universal classes of hash functions,” Journal of Computer and System Sciences, vol.18, pp.143–154, 1979.
[9] T.M. Cover and J.A. Thomas, Elements of Information Theory, 2nd ed., John Wiley & Sons, 2006.
[10] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” IEEE Trans. Inform. Theory, vol.24, no.3, pp.339–348, May 1979.
[11] I. Csiszár and P. Narayan, “Common randomness and secret key generation with a helper,” IEEE Trans. Inform. Theory, vol.46, no.2, pp.344–366, March 2000.
[12] I. Csiszár and P. Narayan, “Secrecy capacities for multiple terminals,” IEEE Trans. Inform. Theory, vol.50, no.12, pp.3047–3061, December 2004.
[13] F. Grosshans, G.V. Assche, J. Wenger, R. Brouri, N.J. Cerf, and P. Grangier, “Quantum key distribution using Gaussian-modulated coherent states,” Nature, vol.421, pp.238–241, January 2003.
[14] T.S. Han, Information-Spectrum Methods in Information Theory, Springer, 2003.
[15] K. Iwata and J. Muramatsu, “An information-spectrum approach to rate-distortion function with side information,” IEICE Trans. Fundamentals, vol.E85-A, no.6, pp.1387–1395, June 2002.
[16] S.K. Leung-Yan-Cheong and M.E. Hellman, “The Gaussian wire-tap channel,” IEEE Trans. Inform. Theory, vol.24, no.4, pp.451–456, July 1978.
[17] Y. Liang, H.V. Poor, and S. Shamai, “Secure communication over fading channels,” IEEE Trans. Inform. Theory, vol.54, no.6, pp.2470–2492, June 2008.
[18] T. Liu and S. Shamai, “A note on the secrecy capacity of the multiple-antenna wiretap channel,” IEEE Trans. Inform. Theory, vol.55, no.6, pp.2547–2553, June 2009.
[19] U. Maurer, “Secret key agreement by public discussion from common information,” IEEE Trans. Inform. Theory, vol.39, no.3, pp.733–742, May 1993.
[20] M. Naito, S. Watanabe, R. Matsumoto, and T. Uyematsu, “Secret key agreement by soft-decision of signals in Gaussian Maurer’s model,” IEICE Trans. Fundamentals, vol.E92-A, no.2, pp.525–534, February 2008. arXive:0804.2940v1.

[21] S. Nitinawarat, "Secret key generation for correlated Gaussian sources," Proceedings of IEEE International Symposium on Information Theory, Toronto, Canada, pp.702–706, July 2008.

[22] Y. Oohama, "Gaussian multiterminal source coding," IEEE Trans. Inform. Theory, vol.43, no.6, pp.1912–1923, November 1997.

[23] L. Ozarow, "On a source coding problem with two channels and three receivers," Bell Syst. Tech. J., vol.59, no.10, pp.1909–1921, December 1980.

[24] D. Slepian and J.K. Wolf, "Noiseless coding of correlated information sources," IEEE Trans. Inform. Theory, vol.19, no.4, pp.471–480, July 1973.

[25] C. Tian and J. Chen, "Remote vector Gaussian source coding with decoder side information under mutual information and distortion constraints," IEEE Trans. Inform. Theory, vol.55, no.10, pp.4676–4680, October 2009.

[26] A.D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol.54, no.8, pp.1355–1387, 1975.

[27] A.D. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," IEEE Trans. Inform. Theory, vol.22, no.1, pp.1–10, January 1976.

Shun Watanabe received the B.E., M.E., and Ph.D. degrees from Tokyo Institute of Technology in 2005, 2007, and 2009 respectively. He is currently an Assistant Professor in the Department of Information Science and Intelligent Systems of University of Tokushima. His current research interests are in the areas of information theory, quantum information theory, and quantum cryptography.

Yasutada Oohama was born in Tokyo, Japan in 1963. He received the B.Eng., M.Eng., and D.Eng. degrees in mathematical engineering from University of Tokyo, Tokyo, in 1987, 1989, and 1992, respectively. From 1992 to 2006, He was with Kyushu University, Fukuoka, Japan. Since 2006 he has been with University of Tokushima, Tokushima, Japan. He is currently a professor at the Department of Information Science and Intelligent Systems. His current research interest includes basic problems in information theory and related areas.